AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

SEP - 8 2017

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
MICROSOFT ACCOUNT:
theheadmaster151@live.com
THAT IS STORED AT PREMISES CONTROLLED BY
MICROSOFT CORPORATION

Case No. 1:17-SW-585

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1030, 1343, 371	See attached Affidavit in Support of Search Warrant.

The application is based on these facts:

SEE AFFIDAVIT.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Reviewed by AUSA/SAUSA:
Kellen Dwyer

Special Agent Gerald Kim, Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/8/17

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

The Honorable Theresa C. Buchanan, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **MICROSOFT ACCOUNT: theheadmaster151@live.com** THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION	Case No. 1:16-sw- **Filed Under Seal**

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with Microsoft account **theheadmaster151@live.com** which is stored at premises owned, maintained, and/or controlled by **MICROSOFT CORPORATION ("Microsoft")** located in Redmond, Washington.

The warrant directed to Microsoft applies to all data and records associated with Microsoft account **theheadmaster151@live.com**, to include all data and information stored on all online, file-hosting and cloud services, such as OneDrive, Live, and Azure offered by Microsoft.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **MICROSOFT ACCOUNT: theheadmaster151@live.com** THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION	Case No. 1:16-sw- **Filed Under Seal**

ATTACHMENT B

Property to be Seized

I. Information to be disclosed by Microsoft (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, passwords, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose all stored communications, records, and other evidence in your possession, to include the following information to the government for each account or identifier listed in Attachment A from account creation to the present:

The contents of any communication or file stored by or for the Accounts and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.

All data and records associated with Microsoft account **theheadmaster151@live.com**, to include all files, data, and information stored on all online, file-hosting and cloud services, such as OneDrive, Live, and Azure offered by Microsoft;

a. an image copy of all data and information electronically stored in the TARGET SERVER pertaining to Microsoft account **theheadmaster151@live.com**;

b. all information in the possession of **Microsoft** that might identify the person or persons who operate, pay for, or are associated with the TARGET SERVER pertaining to Microsoft account **theheadmaster151@live.com**, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), types of services utilized, means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. All records and other information relating to the Accounts and any associated accounts including, but not limited to the following:

a) Full registration and account information, including names, usernames, addresses, phone numbers, and any e-mail addresses
b) SMS Records
c) E-mail and password records
d) Documents
e) Files (to include image files)
f) Descriptions of services subscribed to and service length (with start date)
g) Internet Protocol ("IP") activity logs, including records of session times and durations
h) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, Flash Shared Object, FSO/VID, or any other MacID numbers
i) Payment transactions, including billing records and all financial instruments associated with the account (with full credit card and bank account numbers), including copies (front and back) of checks sent to or from the account holder
j) Correspondence with the account, and all complaints against the account
k) Please identify any other accounts with a common name, address, e-mail address, or Internet Protocol address, and please provide these records for these associated accounts
l) The contents of all other information associated with the account, including basic subscriber information, such as email address, member identification number, data and time stamp of account creation, billing information, snapshot of member profile, IP logs, profile summary, experience and education of member, recommendations, groups, network update stream, user profile photo, IP address, date of account access, visits, member connections, private communications, invitations, messages, and connections, and other data
m) All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files
n) For all accounts that are linked to any of the accounts listed in Attachment A by cookies, secondary or recovery email address or telephone number, provide:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations and IP history log;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), MSISDN, International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Station Equipment Identities ("IMEI"));
7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer fraud), 2 (aid and abet), 1343 (wire fraud), and 371 (conspiracy), from account creation to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Information regarding the administration of the Nitroproducts.info website and the sale and support of malicious software;

2. Records relating to malware executables, including Limitless, Syndicate, and NanoCore, among other malware;

3. Records related to JKBEST22, HeadMaster, and Supporter747, and records relating to the identity of customers and co-conspirators ;

4. Records of customers who have obtained services from JKBEST22, HeadMaster, Supporter747, and nitroproducts.

5. Records related to nitroproducts, nitroproducts.info;

6. Records related to any wire transfers, including online payment providers;

7. Encryption and decryption keys;

8. BitLocker recovery keys;

9. Passwords;

10. All records, documents, programs, applications, or materials related to hacking or methods for gaining access to computers or computer networks, including how to configure or use computer hardware, software, or other related items for purposes of gaining access to computers and computer networks;

11. All records, documents, programs, applications or materials related to exploiting computer software and hardware flaws;

12. All records, documents, programs, applications or materials related to malware or methods for conducting malicious computer activity;

13. All records, documents, programs, applications or materials related to scripts for sending email or scripts for cracking passwords;

14. All records, documents, programs, applications or materials related to locations, communications, or identities of co-conspirators;

15. All records, documents, programs, applications or materials related to locations and identities of other computers used in hacking;

16. All records, documents, programs, applications or materials related to victims of computer hack;

17. All records, documents, programs, applications or materials related to current and past employment;

18. All records, documents, programs, applications or materials related to bank accounts used to receive funds derived from hacking.

19. Records relating to malware executables;

20. Records relating to the dissemination of malicious and fraudulent software;

21. Records relating to configuration files and commands for infected computers;

22. Records relating to the purchase or leasing of, or payment for, computer infrastructure and computer peripherals;

23. Records relating to online and business revenues;

24. Records relating to the dissemination of malicious and fraudulent software;

25. Records relating to configuration files and commands for infected computers;

26. Records relating to instant messaging;

27. Records relating to the purchase or leasing of, or payment for, computer infrastructure and computer peripherals;

28. Records relating to online and business revenues;

29. Records and information relating to who created, used, or communicated with the account, including records about their identities and whereabouts; and

30. Communications with an co-conspirators and information concerning the true identity of those co-conspirators.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

SEP - 8 2017

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **MICROSOFT ACCOUNT: theheadmaster151@live.com** THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION

Case No. 1:17-sw-585

Filed Under Seal

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Gerald Kim, being duly sworn, state:

1. I make this affidavit in support of an application for a search warrant for information associated with Microsoft account **theheadmaster151@live.com** (the "TARGET ACCOUNT") that is stored at premises owned, maintained, and/or controlled by **MICROSOFT CORPORATION ("Microsoft")** located in Redmond, Washington, to disclose certain records and other information pertaining to the Live account **theheadmaster151@live.com**. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been a Special Agent with the Federal Bureau of Investigation for over fourteen years and am currently assigned to the Washington Field Office. As a Special Agent

assigned to a cyber-squad, I have received training in, and am authorized to investigate, crimes involving computers and computer intrusions. Before working at the Washington Field Office, I was a Program Manager at FBI Cyber Headquarters, where I oversaw cyber intrusion investigations at the strategic level. I have received training in, and have participated in, the execution of search warrants and the seizing of evidence, including computer, electronic evidence, and email evidence.

3. The facts in this affidavit are from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, I submit that there is probable cause to believe that violations of Title 18, United States Code, Sections 1030 (computer fraud), 2 (aid and abet), 1343 (wire fraud), and 371 (conspiracy) have been committed by the person using the TARGET ACCOUNT. I submit that there is also probable cause to search the information described in Attachment A for evidence, fruits, and instrumentalities of these crimes, as further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711, 2703(a), (b)(1)(A), (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). The presence of a law enforcement officer is not required for the service or execution of this warrant. 18 U.S.C. § 2703(g).

SUMMARY OF PROBABLE CAUSE

6. The FBI and the Justice Department are investigating a cybercriminal who uses the alias "jkbest22," amongst others, and runs a website called "Nitroproducts.info" that serves as an online marketplace for malicious software ("malware"). The contact for the administrator of Nitroproducts, as listed on its website, was **jkbest22@gmail.com**. The FBI obtained a search warrant for that email address and confirmed that it was, in fact, being used to run the Nitroproducts website, to sell malicious software, and to provide customer support to hackers using the malware to commit computer intrusions. A review of **jkbest22@gmail.com** also provided probable cause to believe that the user of that account also uses the TARGET ACCOUNT and has used the TARGET ACCOUNT to receive payment for the Nitroproducts business. Based on my training and experience, I know that Microsoft email accounts typically contain extensive information, to include travel records, bank records, communications, and photographs that prove the true identity of the account's user. Accordingly, I submit that there is probable cause that the TARGET ACCOUNT contains evidence of the running of the Nitroproducts business, to include payment information, as well as evidence as to the identity of the person running Nitroproducts.

Nitroproducts.info Distributed Malware Known as the Limitless Logger and Syndicate Stealer

7. The developer of the Limitless and Syndicate malware, "Z.S.," pled guilty in this Court to aiding and abetting computer intrusions and is cooperating with the FBI.

8. In connection with his guilty plea, Z.S. admitted that he designed the Limitless and Syndicate keyloggers for the purpose of allowing users to access victim computers without

authorization and steal information of value, such as passwords and other personal information, from the victim computers.

9. One purpose of the keyloggers was to access without authorization sensitive information, such as passwords, on the computers on which the software was installed and send the stolen data to a website or email account designated by its users. The keyloggers offered various features, including, but not limited to, the following:

a. The ability to recover all keystrokes typed on the victim's computer or only custom keystrokes, such as those entered into a web browser;

b. The ability to recover the victim's passwords stored in a web browser; and

c. The ability to resume keylogging every time the victim's computer restarts;

10. The Keylogger was sold to more than one thousand users who, in turn, used the Keylogger to infect thousands of computers. One of the victim computers was identified as being located in the Eastern District of Virginia.

11. Z.S. also admitted that he partnered with "jkbest22" to sell his malicious products on Nitroproducts.info. A review of Z.S. and jkbest22's communications confirms this fact. Z.S. further admitted that he communicated with jkbest22 at the email address **jkbest22@gmail.com**.

Nitroproducts.info Distributed Malware Known as the NanoCore RAT

12. T.H. is another malware developer who pled guilty in this Court to aiding and abetting computer intrusions. T.H.'s malware is called the NanoCore RAT. I have personally observed the NanoCore RAT being offered for sale through Nitroproducts.info.

13. Specifically, the NanoCore RAT is a remote access tool, or "RAT." A RAT is a program designed to allow a computer hacker to take complete control of a victim's computer for the purpose of performing various malicious activities. RATs provide hackers with a

backdoor into the infected system of a victim computer so that the hacker can spy on the victim's computer, cause it to run additional malicious software, or launch attacks on other computer systems. The NanoCore RAT to include a number of malicious features, including the following:

a. A keylogger that allowed NanoCore users to record all keystrokes typed on the victim computer;

b. A password downloader that allowed NanoCore users to steal passwords, such as email and banking passwords, that were saved on the victim computer;

c. A webcam feature that allowed NanoCore users to surreptitiously activate the webcam on the victim computer in order to spy on victms;

d. A file access feature that allows NanoCore users to view, delete, download, and otherwise manipulate files stored on the victim computer.

jkbest22@gmail.com was the Contact Email on the Nitroproducts Website and Was Used To Sell and Support Malware

14. The Limitless Keylogger, Syndicate Stealer, and NanoCore RAT malware products were advertised on the website http://nitroproducts.info. The contact email address listed on the nitroproducts.info website to obtain product support was **jkbest22@gmail.com**. Based on training and experience, this email address would have received support-type questions or questions pertaining to the products offered on the website..

15. I reviewed the website nitroproducts.info which advertised various RATs, Keylogger, Stealer and Crypters. The NanoCore RAT was listed under the category "Windows RAT" with the following description:

Fast Remote Desktop/Webcam/File Manager
Small output size

Steal Bitcoin/Runescape/Browsers/Passwords

The Limitless Logger and Syndicate Stealer were listed under the category "Logger/Stealer" with the following description:

Password Recovery Options
Steal with all latest browsers
Screenshot stealer
Bitcoin/Outlook Stealer & Much More

16. I reviewed the contents of the email account **jkbest22@gmail.com** and the email account used by Z.S. I identified emails pertaining to the sale and customer support for Limitless, Syndicate and NanoCore. Examples are as follows:

a. On 5/19/2014 and 5/20/2014, Arrow Khan <jkbest22@gmail.com> corresponded with Z.S. via email asking each other if there was a problem with the Limitless server.

b. On 1/24/2014, Arrow Khan <jkbest22@gmail.com> sent an email to Z.S. informing Z.S. that a payment of $80 was sent to Z.S. and Arrow Khan made 4 referrals for the Syndicate Logger.

c. On 8/1/2014, Arrow Khan <jkbest22@gmail.com> sent an email to Z.S. notifying Z.S. that a $70 payment was sent. Arrow Khan also provided an update that 48 Syndicate Logger referrals were made.

d. On 10/6/2014, Arrow Khan <jkbest22@gmail.com> and Z.S. corresponded over email regarding a complaint made by a user of Syndicate and Limitless keyloggers.

e. On 11/26/2014, a customer using the email address "mustapha kabiru <mustacrescentegypt@gmail.com>, corresponded with Arrow Khan

(jkbest22@gmail.com) over email. Mustapha Kabiru complained about an issue with a keylogger and requested for a botnet or RAT.

> *I Hope this time around your product will be different. last time you gave me a shitty keylogger..ran support couple of times and disappeared.*
> *I need botnet. or any good RAT*

In response, Arrow Khan provided the website link "http://nitroproducts.info/red/protector.html" and suggested the NanoCore RAT.

f. On 12/1/2014, a customer using the email address "tele talk <teletalk@yandex.ru>" corresponded with Arrow Khan (jkbest22@gmail.com) via email. "Tele Talk" asked where he would "get result of victim." Arrow Khan's response to the question was from the RAT.

> *On ur rat*
> *Nanocore*
> *Be sure u need to connect vpn before using rat*

Probable Cause that the User of jkbest22@gmail.com also Uses the TARGET ACCOUNT and Has Received Nitroproduct Payments at the TARGET ACCOUNT

17. Google provided the subscriber information for **jkbest22@gmail.com** which was created on January 1, 2009 and the recovery email account listed was **theheadmaster151@live.com**. Based on my training and experience, I know that users are supposed to, and typically do, provide another email address they control as their recovery email address. This is because the entire point of a recovery email address is to be able to access your primary email address in the event you are locked out of it.

18. **Jkbest22@gmail.com** also signed emails as "HeadMaster," further indicating that the TARGET ACCOUNT is his.

19. The historical usage records for jkbest22@gmail.com revealed emails from unknown persons with different email accounts that were sent to the TARGET ACCOUNT in 2015, 2016, and 2017 were also delivered to jkbest22@gmail.com.

20. I reviewed the Google chats between jkbest22@gmail.com and omoayeent@gmail.com. The individual using the email account omoayeent@gmail.com messaged jkbest22@gmail.com regarding an email he sent informing of the payment he made for a one month use of the Infinity Crypter. In response, jkbest22@gmail.com asked for the email address to which omoayeent@gmail.com sent regarding the payment notification. Omoayeent@gmail.com provided three email addresses, including the TARGET ACCOUNT. Subsequently, jkbest22@gmail.com provided a key (a string of alpha-numeric characters) for omoayeent@gmail.com to download the crypter.

Probable Cause to Search the SUJECT ACCOUNT

21. I submit that there is probable cause to believe that the TARGET ACCOUNT contains evidence of a scheme to aid and abet computer intrusions, in violation of 18 U.S.C. §§ 1030 and 2. In particular, I submit that there is probable cause that the TARGET ACCOUNT contains evidence of the running of the Nitroproducts business, to include payment information, as well as evidence as to the identity of the person running Nitroproducts.

BACKGROUND ON EMAIL

22. **Microsoft** provides information infrastructure platform in the cloud on a server and has data center locations, including in the United States, where account holders can store information. In general, providers like **Microsoft** ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail

addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

23. A server is a computer, connected to the Internet that provides services to other computers. A web server, for example, sends web pages to a user's computer when a user requests those web pages. Customers can connect from their own computers to the server computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special web site interface offered by a web hosting company. It is frequently also possible for the customer to directly access the server computer through the Secure Shell ("SSH") or Telnet protocols. These protocols allow remote users to type commands to the server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses ("IP addresses") of the remote users' computers (IP addresses are used to identify

computers connected to the Internet). Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

24. **Microsoft** maintain server computers connected to the Internet. Through a variety of possible arrangements, Microsoft sells to customers the right to use their server computers and other services. In these shared-hosting arrangements, individual customers may each upload their own data and programs and may edit and delete their own data, but often may have limited access to other users' data. In this case, this search warrant only seeks information associated with particular Microsoft account **theheadmaster151@live.com** so that information from other unrelated customers is unlikely to be seized.

THE NATURE OF EXECUTION

25. **Microsoft** has either physical access to the TARGET SERVER hosting Microsoft account **theheadmaster151@live.com** or electronic access to data stored on the TARGET SERVER, or both. Moreover, Microsoft provides Internet connectivity to the servers at its facility. Thus, I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government records. Specifically, **Microsoft** will be compelled to disclose copies of the records and other information particularly described in Section I of Attachment B. Government agents will serve this warrant on **Microsoft**, perhaps delivering the warrant in person. It is possible that Microsoft will request the assistance of the government in making the necessary copies; if asked for such assistance, the government will likely provide it.

26. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. The examination may require techniques, including but not limited to computer-assisted scans, that might expose many parts of the data to human inspection in order to determine whether it is evidence described by the warrant.

27. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. However, I expect that government agents will offer to assist **Microsoft** in the task of complying with this warrant, including by making the necessary copies of data. **Microsoft** will be free to decline that assistance, but is compelled to disclose the data regardless.

CONCLUSION

28. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations, or attempted violation, of Title 18, United States Code, Sections 1030 (computer fraud), 2 (aid and abet), 1343 (wire fraud), and 371 (conspiracy) may be located in the TARGET ACCCOUNT described in Attachment A. I request that the Court issue the proposed search warrant for the TARGET ACCOUNT to require Microsoft Corporation to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Government-authorized persons will then review that information to locate the items described in Section II of Attachment B.

Respectfully submitted,

Gerald Kim, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on September 8, 2017

/s/
Theresa Carroll Buchanan
United States Magistrate Judge

The Honorable Theresa C. Buchanan
United States Magistrate Judge
Alexandria, Virginia

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **MICROSOFT ACCOUNT: theheadmaster151@live.com** THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION	Case No. 1:16-sw- **Filed Under Seal**

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with Microsoft account **theheadmaster151@live.com** which is stored at premises owned, maintained, and/or controlled by **MICROSOFT CORPORATION ("Microsoft")** located in Redmond, Washington.

The warrant directed to Microsoft applies to all data and records associated with Microsoft account **theheadmaster151@live.com**, to include all data and information stored on all online, file-hosting and cloud services, such as OneDrive, Live, and Azure offered by Microsoft.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **MICROSOFT ACCOUNT: theheadmaster151@live.com** THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORPORATION	Case No. 1:16-sw- **Filed Under Seal**

ATTACHMENT B

Property to be Seized

I. Information to be disclosed by Microsoft (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, passwords, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose all stored communications, records, and other evidence in your possession, to include the following information to the government for each account or identifier listed in Attachment A from account creation to the present:

The contents of any communication or file stored by or for the Accounts and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.

All data and records associated with Microsoft account **theheadmaster151@live.com**, to include all files, data, and information stored on all online, file-hosting and cloud services, such as OneDrive, Live, and Azure offered by Microsoft;

a. an image copy of all data and information electronically stored in the TARGET SERVER pertaining to Microsoft account **theheadmaster151@live.com**;

b. all information in the possession of **Microsoft** that might identify the person or persons who operate, pay for, or are associated with the TARGET SERVER pertaining to Microsoft account **theheadmaster151@live.com**, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), types of services utilized, means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;

c. All records and other information relating to the Accounts and any associated accounts including, but not limited to the following:

a) Full registration and account information, including names, usernames, addresses, phone numbers, and any e-mail addresses
b) SMS Records
c) E-mail and password records
d) Documents
e) Files (to include image files)
f) Descriptions of services subscribed to and service length (with start date)
g) Internet Protocol ("IP") activity logs, including records of session times and durations
h) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, Flash Shared Object, FSO/VID, or any other MacID numbers
i) Payment transactions, including billing records and all financial instruments associated with the account (with full credit card and bank account numbers), including copies (front and back) of checks sent to or from the account holder
j) Correspondence with the account, and all complaints against the account
k) Please identify any other accounts with a common name, address, e-mail address, or Internet Protocol address, and please provide these records for these associated accounts
l) The contents of all other information associated with the account, including basic subscriber information, such as email address, member identification number, data and time stamp of account creation, billing information, snapshot of member profile, IP logs, profile summary, experience and education of member, recommendations, groups, network update stream, user profile photo, IP address, date of account access, visits, member connections, private communications, invitations, messages, and connections, and other data
m) All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files
n) For all accounts that are linked to any of the accounts listed in Attachment A by cookies, secondary or recovery email address or telephone number, provide:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations and IP history log;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), MSISDN, International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Station Equipment Identities ("IMEI"));
7. Other subscriber numbers or identities (including temporarily assigned network addresses and registration IP addresses (including carrier grade natting addresses or ports)); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer fraud), 2 (aid and abet), 1343 (wire fraud), and 371 (conspiracy), from account creation to present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Information regarding the administration of the Nitroproducts.info website and the sale and support of malicious software;

2. Records relating to malware executables, including Limitless, Syndicate, and NanoCore, among other malware;

3. Records related to JKBEST22, HeadMaster, and Supporter747, and records relating to the identity of customers and co-conspirators ;

4. Records of customers who have obtained services from JKBEST22, HeadMaster, Supporter747, and nitroproducts.

5. Records related to nitroproducts, nitroproducts.info;

6. Records related to any wire transfers, including online payment providers;

7. Encryption and decryption keys;

8. BitLocker recovery keys;

9. Passwords;

10. All records, documents, programs, applications, or materials related to hacking or methods for gaining access to computers or computer networks, including how to configure or use computer hardware, software, or other related items for purposes of gaining access to computers and computer networks;

11. All records, documents, programs, applications or materials related to exploiting computer software and hardware flaws;

12. All records, documents, programs, applications or materials related to malware or methods for conducting malicious computer activity;

13. All records, documents, programs, applications or materials related to scripts for sending email or scripts for cracking passwords;

14. All records, documents, programs, applications or materials related to locations, communications, or identities of co-conspirators;

15. All records, documents, programs, applications or materials related to locations and identities of other computers used in hacking;

16. All records, documents, programs, applications or materials related to victims of computer hack;

17. All records, documents, programs, applications or materials related to current and past employment;

18. All records, documents, programs, applications or materials related to bank accounts used to receive funds derived from hacking.

19. Records relating to malware executables;

20. Records relating to the dissemination of malicious and fraudulent software;

21. Records relating to configuration files and commands for infected computers;

22. Records relating to the purchase or leasing of, or payment for, computer infrastructure and computer peripherals;

23. Records relating to online and business revenues;

24. Records relating to the dissemination of malicious and fraudulent software;

25. Records relating to configuration files and commands for infected computers;

26. Records relating to instant messaging;

27. Records relating to the purchase or leasing of, or payment for, computer infrastructure and computer peripherals;

28. Records relating to online and business revenues;

29. Records and information relating to who created, used, or communicated with the account, including records about their identities and whereabouts; and

30. Communications with an co-conspirators and information concerning the true identity of those co-conspirators.